

REMARKS

Claims 1 - 33 are in this Application. Applicant has amended claim 5 and added new claims 9 - 33 to clarify claim scope. No new matter has been added. In the Office Action mailed on April 9, 2001, the Examiner rejected claim 1 pursuant to 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 4,484,027, filed November 19, 1981, and issued to Lee et al. (Lee). The Examiner rejected claim 5 pursuant to 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,517,567, filed August 23, 1994, and issued to Epstein (Epstein). The Examiner rejected claims 2-4 pursuant to 35 U.S.C. §103(a) as being anticipated by Lee in view of U.S. Patent No. 6,070,058, filed November 10, 1977, and issued to Waldroup et al. (Waldroup). The Examiner rejected claims 6 and 8 pursuant to 35 U.S.C. §103(a) as being anticipated by Lee in view of Waldroup. Applicant respectfully traverses the Examiner's rejections.

35 U.S.C. §102(b): Lee

The Examiner rejected independent claim 1 pursuant to 35 U.S.C. § 102(b) as being anticipated by Lee.

In regards to claim 1, the office action contends that Lee teaches each and every element of Applicant's claimed invention. Applicant respectfully disagrees. Applicant's claim 1 reads:

A method for generating random data bits in wireless communications device, comprising the steps of:

processing a received signal; and
extracting said random data bits from said processed receive signal.

The office action cites Lee Fig. 1, #36, 34 as anticipating Applicant's invention as claimed in claim 1. Specifically, the office action argues that "Lee teaches processing a

received signal and extracting random data bits from the processed receive signal.” (See Office Action, Detail 1.) Applicants respectfully disagree.

First, Lee does not disclose processing a received signal and extracting random data bits from the processed received signal. Lee discloses a method of using a private/public key pair to scramble transmitted cable television signals. The scrambling keys are generated by matching random number generators in the transmitter and the receiver. The receiver of Lee is not a wireless communications device. Rather, it is a cable box that sits on top of a TV connected to a coaxial cable. The cable box receiver does not generate the private portion of the key pair from the received video. Rather, the cable box recreates the private key necessary to descramble the received video by starting the matching random number generator off with the same seed as the transmitter. (See Column 1 – Column 3.) Fig. 1 shows a random number, or key, generator in the transmitter and a decipherer to regenerate the key in the receiver. However, Lee teaches away from Applicant’s claimed invention by using known seed information, which is pseudo-random rather than truly mathematically random to create the key for descrambling a received cable signal, while Applicant discloses extracting truly random data bits from the processing of a received signal in order to encrypt a transmitted signal in a wireless communications system.

Applicant respectfully submits that the only commonality between Applicant’s claimed invention and the cited art is a component named random number generator in a figure of the cited art. Furthermore, the random number generator of the figure does not perform the functionality claimed in Applicant’s claim 1 and is used in an unrelated context. Lee does not teach extracting mathematically random data bits from a processed receive signal to encrypt a signal for wireless transmission as disclosed by Applicant. Lee discloses seeding a random number generator to generate a pseudo-random number for descrambling a cable TV signal.

In response to the examiner’s statement that the examiner disagrees with the way the claim is drafted because “the receiver does not recite randomly extracting data bits from the received signal. The examiner asserts that a random number is in effect random data bits because the number is composed of data bits” (Detail 8), Applicant

respectfully submits that the comment is irrelevant because, as detailed above, Lee does not disclose extracting anything from the received signal to recreate a random number.

Consequently, because Lee fails to teach each and every element of Applicant's invention as claimed in claim 1, Lee fails to anticipate and the examiner is respectfully requested to withdraw the rejection of claim 1.

35 U.S.C. §102(b): Epstein

The Examiner rejected independent claim 5, pursuant to 35 U.S.C. § 102(b) as being anticipated by Epstein.

In regards to claim 5, the office action contends that Epstein teaches each and every element of Applicant's claimed invention. Applicant respectfully disagrees. Applicant's claim 5 reads:

An encryption system, comprising:

a random number selector subsystem for generating random numbers from data bits generated from random received signal characteristics that are extracted from the received signal using existing wireless phone hardware; and

an encryptor for encrypting a signal using said random numbers.

The office action cites Epstein element #202 as anticipating Applicant's invention as claimed in claim 5. Specifically, the office action argues that "In claim 5, Epstein disclose use of a random number generator #202 as part of element #200; the wireless device. As device #202 is part of a wireless device, the bits are generated for use by device #202 are in effect generated by the wireless device. Hence, generating a random numbers from data bits generated from existing wireless phone hardware and encryptor for encrypting a signal using said random numbers are disclosed by Epstein in (col. 2, lines 61-67; col. 3, lines 45-50)." (See Office Action, Detail 2.) Applicants respectfully disagree.

Applicant respectfully submits that the examiner's argument that Applicant's invention is anticipated by Epstein is flawed in the same manner as the argument that Applicant's invention is anticipated by Lee. Like Lee, Epstein teaches a key based DES encryption system where encryption keys are generated by pseudo-random number generators. (See Col.1, lines 25-53.) The random number generators are pseudo random and they do not use truly random received signal characteristics to extract random data bits from the received signal. Epstein teaches away from Applicant's claim 5 by disclosing a method for securely transferring pseudo-random encryption keys between transmitters and receivers rather than generating random numbers at a receiver by extracting truly random data from mathematically random characteristics of the received signal.

Consequently, because Epstein fails to teach each and every element of Applicant's invention as claimed in claim 5, Epstein fails to anticipate and the examiner is respectfully requested to withdraw the rejection of claim 5.

35 U.S.C. §103(a): Lee in view of Waldroup

The Examiner rejected claims 2-4 pursuant to 35 U.S.C. §103(a) as being anticipated by Lee in view of Waldroup. In view of the arguments detailed above with respect to independent claim 1, Applicant submits that dependent claims 2-4 constitute patentable subject matter in view of the cited reference.

35 U.S.C. §103(a): Epstein in view of Waldroup

The Examiner rejected claims 6 and 8 pursuant to 35 U.S.C. §103(a) as being anticipated by Epstein in view of Waldroup. In view of the arguments detailed above with respect to independent claim 5, Applicant submits that dependent claims 6 and 8 constitute patentable subject matter in view of the cited reference.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicants submit that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application is earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: 07/09/2002

By: Maryanne E. DeAngelo
Maryanne E. DeAngelo
Agent for Applicant
Registration No. 47,228

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 651-2384
Facsimile: (858) 658-2502

APPENDIX A

5. An encryption system, comprising:
- a random number selector subsystem for generating random numbers from data bits generated [by] from random received signal characteristics that are extracted from the received signal using existing wireless phone hardware; and
 - an encryptor for encrypting a signal using said random numbers.